

Context-Independent Centrality Measures Underestimate the Vulnerability of Power Grids

Trivik Verma^{1,2,3}, Wendy Ellens², and Robert E. Kooij^{1,2}

¹ Delft University of Technology, EEMCS, The Netherlands

² Performance of Networks and Systems, TNO, The Netherlands

³ Institut f. Baustoffe (IfB)/ETH Risk Center, Zurich, Switzerland

Abstract. Power grids vulnerability is a key issue in society. A component failure may trigger cascades of failures across the grid and lead to a large blackout. Complex network approaches have shown a direction to study some of the problems faced by power grids. Within Complex Network Analysis structural vulnerabilities of power grids have been studied mostly using purely topological approaches, which assumes that flow of power is dictated by shortest paths. However, this fails to capture the real flow characteristics of power grids. We have proposed a flow redistribution mechanism that closely mimics the flow in power grids using the Power Transfer Distribution Factor (PTDF). With this mechanism we enhance existing cascading failure models to study the vulnerability of power grids.

We apply the model to the European high-voltage grid to carry out a comparative study for a number of centrality measures. ‘Centrality’ gives an indication of the criticality of network components. Our model offers a way to find those centrality measures that give the best indication of node vulnerability in the context of power grids, by considering not only the network topology but also the power flowing through the network. In addition, we use the model to determine the spare capacity that is needed to make the grid robust to targeted attacks. We also show a brief comparison of the end results with other power grid systems to generalise the result.

Keywords: power grids, complex networks, cascading failures, flow redistribution, centrality, tolerance parameter, vulnerability

1 Introduction

Power grids are the backbone of modern society. A power grid is a network of generation, transmission and distribution sub-stations that transmit power to households and local businesses. Energy is transferred through high-voltage transmission lines in order to reduce losses over large distances. The evolution of high-voltage grids has been influenced by social, technical, economic, political and environmental decisions that favour economic prosperity, security and quality of life. A disruption in the functioning of power grids can have severe impact

on the social welfare of society (Bompard et al. 2007). The reliability of power grids is thus very critical for optimal functioning of society.

In recent decades a lot of blackouts have been experienced by power grids across the world (McLinn 2009). Power outages are consequences of perturbations that overload the entire system by spreading flows across the network. These perturbations range from severe weather conditions to several human errors. Failure of a component in the power grid may cause some power to be redirected to its neighbours, which in turn may get overloaded and redirect power to *their* neighbours causing them to fail. These failures may initially start with any component of the power grid (faults at power station, transmission lines, defects in the distribution network or even a small short-circuit) that propagates its effects to its direct neighbours and so on. This effect is called a *cascading failure*.

Like most complex networks, power grids are also made up of small components that act in a simple manner and together give rise to a behaviour that emerges complex in nature (Mitchell 2009). As the size of power grids is increasing over the years, it is becoming very important to understand the emergent behaviour of such systems. The question still remains how complex and vulnerable these systems are and how the small simple components give rise to a larger complex mesh of power. Analysing vulnerability of power grids is a significant issue in society and much has been contributed towards such efforts (Albert et al. 2004, Bompard, Napoli & Xue 2009, Bompard, Napoli & Xue 2010, Bompard, Wu & Xue 2010, Bompard et al. 2007, Bompard, Maserà, Napoli & Xue 2009, Crucitti et al. 2004, Kinney et al. 2005, Koç et al. 2013, Simonsen et al. 2008). These discussions give rise to an interesting direction of research that not only deals with topological (purely relating to the structure and interconnection pattern of the grid) vulnerability but also looks into the load flows of power grids (Arianos et al. 2009, Crucitti et al. 2004, Kinney et al. 2005, Nasiruzzaman & Pota 2011, Youssef et al. 2011).

Disruptions (accidents, human errors, component failures, etc.) in a power grid may lead to a failure that propagates through the grid and results in a large-scale power outage. This cascading failure phenomenon has been researched extensively (Bompard, Napoli & Xue 2009, Crucitti et al. 2004, Kinney et al. 2005, Pahwa et al. 2010, Simonsen et al. 2008, Van Eeten et al. 2011, Youssef et al. 2011) but many properties of power grids are still missing from the analyses and need to be included for a more accurate study. This leads us to study cascading failures by incorporating properties of flows in power grids in order to deal with the problem of power outages in high-voltage power grids. Through this study we want to identify the most *vulnerable* nodes in high-voltage power grids (whose removal causes most damage to the grid) and find out how much capacity is required at each node so that the power grid sustains attacks and failures. More concretely we want to answer two questions: 1) which measure of centrality in complex networks gives the best indication of node vulnerability in power grids and 2) what should be the minimal node *tolerance level* (node capacity relative to the typical loading level) in order to prevent cascading failures that have impact on more than ten percent of the energy delivery.

To answer these questions, we need to predict the evolution of cascading failures in a high-voltage power grid with more accuracy than existing theoretical Complex Network Analysis (CNA) models. The existing cascading failure models (Crucitti et al. 2004, Kinney et al. 2005) assume that power flows between two nodes via the shortest path that exists between them and a few others deal with Direct Current (DC) flow analysis incorporating a dynamic behaviour in the model (Koç et al. 2013, Youssef et al. 2011). It is of little significance whether the length of the shortest path is based on distance or impedance of each link in a path. Power, in reality, flows through multiple paths that exist between two nodes and is divided between these paths based on electrical properties (impedance, conductance, capacitance) of the transmission links as depicted in Fig. 1. Hence, we propose a model with a more realistic flow redistribution mechanism and use it to simulate cascading failures. We trigger a cascading failure by removing a node with the highest centrality (Boccaletti et al. 2006) according to four different centrality measures to find out which removal is the most disruptive and to know which measure best captures the vulnerability of nodes to cascading failures. Thereafter, in the second phase, we perform a new set of cascading failure simulations for different values of the tolerance level by deleting the most vulnerable node according to the centrality in the first phase. This second set of simulations is aimed at finding the minimal tolerance level needed to prevent high-impact cascading failures.

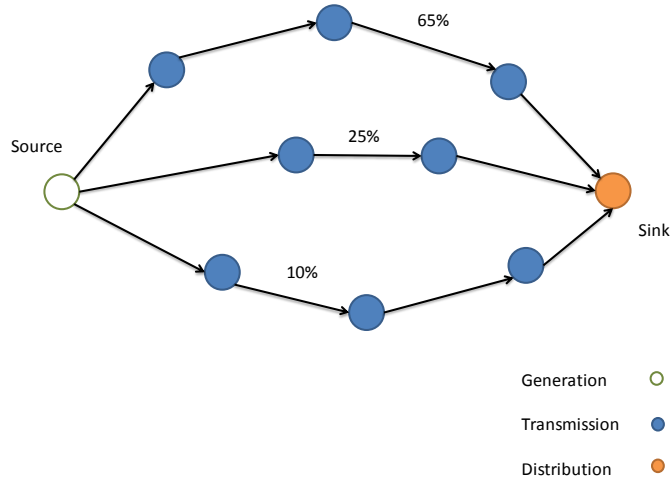


Fig. 1. A network diagram showing the distribution of power across multiple paths between a pair of generation and distribution nodes of a power grid.

The next section, Sect. 2, talks about the context in which this work is carried out. In Subsect. 2.1 we describe literature in which power grids are studied from a complex networks point of view, while Subsect. 2.2 explains the basis for our proposed flow redistribution mechanism. In Sect. 3, we describe our cascading failure model and its constituent parts in detail. Section 4 is about the simulations. We start by defining the settings for our simulations. Next, we talk about the performance measures that are used to quantify the vulnerability of power grids in case of cascading failures. The section continues with a description of the simulation approach and finishes with a discussion of the simulation results. Section 5 marks the end of this article with a short summary and focal points of this research. It also explains future potential that emerges from this work.

2 Related Work

2.1 Complex Network Analysis

This section is dedicated to the relevant work carried out in the field of power grids and cascading failures. We describe summaries of some relevant papers in detail and focal points of each work that might be useful for expanding our model.

Researchers initially focussed on static failures in complex networks (Albert et al. 2004, Albert et al. 2000, Callaway et al. 2000, Cohen et al. 2000). These include the removal of certain components of a network and thereby evaluating the drop in performance of such a network. However, many infrastructure networks like the transport grid/gas pipelines may lose a sizeable part of their performance after a static failure and cause an overload in other parts of the network leading to a partial or complete disruption of facilities. This redistribution of flows led to development of dynamical approaches (Crucitti et al. 2004, Motter & Lai 2002) and their application to more real-world networks.

Next we talk about a dynamic model of cascading failures for complex networks: Crucitti-Latora-Marchiori (CLM) model, by Crucitti et al. (2004). They build a simple model to show how small triggers could lead to catastrophic events in infrastructure networks. The model explains redistribution of flows within the network upon break down of a single node. They show that the collapse of a single node with the highest load is sufficient to considerably lower the efficiency of the entire network.

The CLM model has been adapted to the North American high-voltage power grid by Kinney et al. (2005). The north American power grid is one of the most complex technological networks and transmits electricity but also failures to many parts of the grid. They modelled the grid with certain assumptions about how the load is transferred from one transmission substation to another. Their results suggest that a breakdown of transmission sub-stations could lead up to a loss of 25% of efficiency by spreading flows across the network. Furthermore, they found out that disruption of 40% of the transmission sub-stations lead to cascading failures.

Considerable work has been carried out by researchers in the field of cascading failures in the direction of stationary network load models. The above mentioned studies have that feature in common. Simonsen et al. (2008) have taken a step further and studied the transient dynamics of power systems caused by an initial shock in the network. They have justified their work by the fact that loads have oscillations while adjusting to the new structure of the network and some parts may breakdown before the network stabilises again. The lack of a dynamic load model greatly overestimates the robustness of the network. Furthermore, they conclude that using stationary network load models might predict a different failure sequence for the network far from reality.

Until now we have discussed literature that marks direct application of context-independent concepts and measures from CNA to power grids. Power grids cannot be encapsulated by generic properties of a complex network. Bompard, Maserà, Napoli & Xue (2009) have done major work in exploring the shortcomings of generic application and designing new methodologies to study power grids more efficiently.

In (Bompard, Napoli & Xue 2009) they analyse the structural vulnerabilities of power grids by extending the topological approach to include the physical operative state of the grid in terms of the flows distributing in the links. The authors designed new metrics such as *entropic degree* and *net-ability* and compared them with the traditional purely topological metrics. Entropic degree takes into account not only the number of connections a node has but also the distribution of weights around these connections. It provides a fairly quantitative measurement of the importance of sub-stations in a power grid. Net-ability describes how efficiently power flows over the lines of a transmission grid from supply to demand side. They further extended the topological approach to incorporate several other features of a power grid such as line flow limits, flow paths and demand/supply distribution (Bompard, Napoli & Xue 2010). *Path redundancy* quantifies the available redundancy of paths in transmitting power from generation to distribution sub-stations using the concept of entropy. In case of a cascading failure, *Survivability*, based on path redundancy and net-ability, measures the effectiveness of a grid to match demand with the generation.

On the lines of extending topological approach to analyse power grids, Bompard, Wu & Xue (2010) formulated an electrical betweenness based approach that captures the specific properties of power grids in more detail. This metric focusses on the impedances of the transmission lines. They compared this with the traditional betweenness metric for IEEE bus networks and found that this traditional centrality measure underestimates the vulnerability of power grids.

Centrality is the backbone for identifying critical components in a complex network. Tutzauer (2007) proposed a centrality measure based on entropy that characterises networks with flow along multiple paths. His motivation lies in the idea that centrality measures must be related to the underlying network properties. Very often, researchers use centrality measures to validate models for a particular type of network that may have flow characteristics different from the ones assumed by the measure. Borgatti (2005) points out that this

implicit assumption about the flow characteristics of network may give rise to misleading results.

Koç et al. (2013) have designed a context-dependent centrality measure to assess the importance of nodes in a power grid. The measure describes the significance of a node based on the amount of power flowing through that node to its neighbours. *Node Significance* is a directed and weighted measure and a good estimate of the robustness of a node in a power grid.

Bompard’s seminal work may have inspired optimisation of distributed flows in power grids from a design perspective. Asztalos et al. (2012) used an edge weighting scheme to optimise the flow efficiency and robustness of scale-free networks to cascading failures. They studied models where flow is distributed and initiates from all paths between a pair of source and sink nodes.

Van Eeten et al. (2011) illustrate the importance of energy networks. They carry out empirical investigations in the interdependencies of critical infrastructures. Their work involves analysing data from news reports and correlations between cascading failures across different infrastructures. Their findings were rather focused on two domains: telecommunications and energy. Most cascades have propagated from energy networks to telecommunications and there is no sign of a bidirectional relationship.

Power grids have been around for almost two centuries and the continuing complex interconnection patterns have made them more liable to disruptions. Pahwa et al. (2010) have explored mitigation strategies against cascading effects and agreed upon the use of distributed renewable energy sources for decreasing the load on power grids. Subsequently, Youssef et al. (2011) have also explored robustness measures of power grids with respect to cascading failures using a DC power flow model.

2.2 Power Flows

In a power grid, flow between a pair of source and sink nodes does not follow the shortest path between them. Power follows a distributed path based on many system properties (impedance, conductance, capacitance) that impose certain limits on the capacity of these paths (Bompard, Napoli & Xue 2009). Every path that constitutes the flow from source A to sink B is made of several links each. These links have different parameters and each path may contribute a different proportion of power to the flow from source A to sink B.

The amount of information flowing between a pair of nodes is reflected by the shortest path between the nodes (Albert et al. 2004, Crucitti et al. 2004, Rosas-Casals et al. 2007). Contrary to this assumption, in power engineering, electric current (the information flowing in power grids) follows multiple paths between a pair of nodes. Merely using simplified measures from the theory of CNA for defining flow redistribution in a power grid is not enough. The flow in a power grid can be represented in essence by the PTDF.

The Power Transfer Distribution Factor (PTDF) (Dobson et al. 2001) describes the sensitivity of each transmission link to power injection at a particular node and withdrawal at a reference node. This reference node is also known as

Slack. If the slack node is missing, then a generator node with the highest real power is chosen as slack for the system.

PTDF of a component T for a flow between source A and sink B reflects the percentage of power that flows through that component T. For instance, when component Z (part of a path between A and B) has a PTDF of 0.2 for a transfer from A to B, then a transfer of 100 MW from A to B would result in an increase of 20 MW at component Z. On the other hand, if the same factor is -0.2 , then this transfer would result in a decrease of 20 MW at component Z. This implies that for calculating the PTDF of a transmission link, the source and sink nodes must be specified. In the absence of a sink, the reference node acts as the sink that demands the injection at source in the first place. PTDFs are very useful for analysing the change in load at a particular transmission link and identifying the links that might overshoot their capacity.

For a network with N nodes and K transmission links, the PTDF matrix is given by,

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ & & \ddots & \\ a_{K1} & a_{K2} & \dots & a_{KN} \end{bmatrix}, \quad (1)$$

where A is a $K \times N$ matrix and a_{ij} is the change in power of link i when 1 unit of power is injected at node j and withdrawn at the slack node.

The PTDF of a transmission link i for a flow between a pair of nodes g and d can be defined using (1) and the slack node as follows,

$$\rho_i^{gd} = a_{ig} - a_{id}, \quad (2)$$

where ρ_i^{gd} is the change in power of link i when 1 unit of power is injected at node g and withdrawn at node d .

Computation of the PTDF matrix requires a model to calculate load flows and in most cases a DC model of power flow (Dobson et al. 2001) is used. DC power flow models are widely used by the power engineering sector to compute load flows for high-voltage transmission grids. Their reliability has been long questioned and not completely accepted for all application purposes but it is nonetheless a good approximation of active power flows and usually gives values close to $\pm 5\%$ (Purchala et al. 2005) as long as the conditions forming the basis of the method are met with. For a high voltage transmission grid, the conditions for a DC model are satisfied (Purchala et al. 2005).

3 Model

The cascading failure model that we have designed for simulating a high-voltage power grid has three distinct parts, namely input, redistribution and output illustrated in Fig. 2. We explain these parts in the following three subsections.

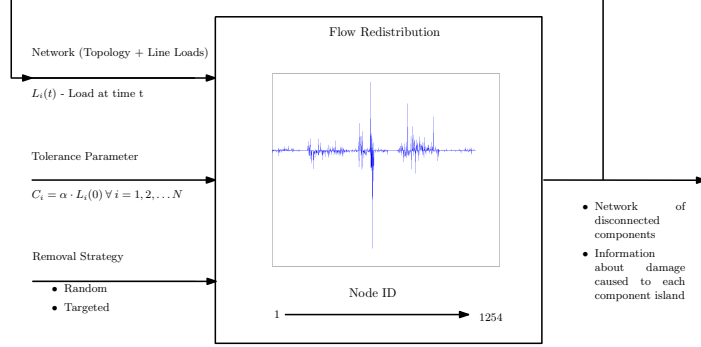


Fig. 2. Scheme showing the constituent parts of the cascading failure model. Left is the input, in the middle is the flow redistribution and to the right is the output. The process is iterated until no more changes, i.e. there is no more flow redistribution and no more nodes are removed because of overloading.

3.1 Input

The input settings for our model consists of the tolerance parameter, the network model and the removal strategy.

Tolerance parameter α

Capacity is a characteristic property of each node/link in any network and it dictates the maximum load a node/link can withstand. Naturally, we will assume that capacity C_i of a node i is directly proportional to its initial stable load $L_i(0)$ (Motter & Lai 2002) at the start of the simulation (time $t = 0$). It is defined as follows,

$$C_i = \alpha \cdot L_i(0) \quad \forall i = 1, 2, \dots, N, \quad (3)$$

where $L_i(0)$ is the current power flowing through each node at the moment when a DC power flow solution was calculated. This proportionality coefficient $\alpha \geq 1$ is the tolerance parameter that marks an upper bound on the load that can flow through each node at any time during the simulation. α is technology dependent, i.e. it cannot be an unreasonably high value.

From (3), it is evident to state the following relation between the tolerance parameter and loading level which is a more inherently natural concept to grasp,

$$\alpha = \frac{100}{ll}, \quad (4)$$

where,

α is the tolerance parameter and ll is the loading level expressed as a percentage.

The relation in (4) implies that when the loading level is say 50%, the tolerance parameter will be $\alpha = 2$, i.e. the network can handle twice its initial load

at each node.

Network Model

High-voltage transmission grid data is used (UCTE n.d.). It has 1254 nodes and 1944 directed links. The network has the following characteristics,
average clustering coefficient $\langle C \rangle = 0.0126$
diameter $d = 48$
average path length $\langle l \rangle = 17.28$

The degree and betweenness distributions of this network are plotted in Fig. 3.

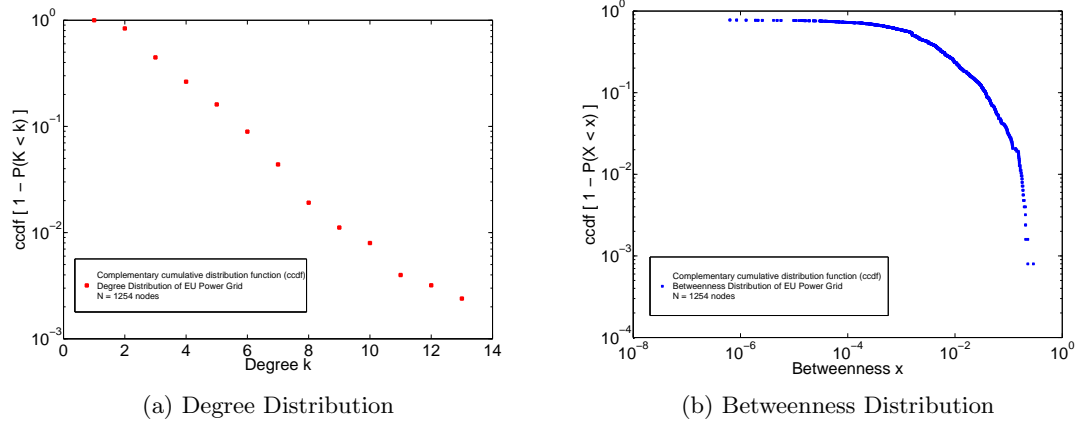


Fig. 3. Degree and Betweenness distributions of EU power grid. The topology of this network is considered undirected and unweighted for these distributions.

This network data consists of the topology of the network, the demand and supply parameters at each generation and load station, and node voltages. A DC power flow solution with all these parameters gives an approximate amount of power flowing through all the high-voltage transmission links of the grid. These load values act as weights in our analysis. This is a stable snapshot of the system that we use for future modelling and simulation purposes.

The DC power flow solution comes from a MATLAB package called MATPOWER (Zimmerman n.d.). The calculation of PTDF matrices is also a part of this package. It is used for modelling the power grid as a network to solve power flow equations and carry out other power flow computation problems.

Removal Strategy

The cause for redistribution of flows in a power grid is due to a component failure or shut-down. In order to simulate the network for cascading failures we have

to remove a node from the network to trigger the redistribution of flows. This removal can either be *Random* or *Targeted*. By removing the most *important* (centrality (Boccaletti et al. 2006)) node from the network we can estimate the worst case damage caused to a power grid due to cascading failures. Nodes of the power network are considered to shut down irreversibly, i.e. once they are switched off during the simulation of a cascading failure (whether due to a failure being propagated or a safeguarding strategy to cut-off a part of the network) they are assumed to be dead for the remaining period of the simulation. We made this choice because of the fact that this work aims at a short interval of time which is conceived from a fault in the network, resulting in a power outage in a matter of seconds.

We included three measures from the theory of CNA that are applicable to all generic network topologies. These are as follows,

- Betweenness Centrality (undirected, unweighted)
- Degree Centrality (undirected, unweighted)
- Closeness Centrality (undirected, unweighted)

And one measure specifically designed for power grids called *Node Significance* (directed, weighted) explained previously in Sect. 2.1.

These measures provide us with information about the importance of a node in a network with respect to the network itself. We take only undirected and unweighted *traditional* measures to emphasize on the context-independent part of our study.

On the basis of the above discussion we form the following five strategies for node removal which trigger a cascading failure,

1. Betweenness based removal
2. Degree based removal
3. Closeness based removal
4. Node Significance based removal
5. Random removal

1-4 belong to the targeted removals and are based on the importance of a node within a network. A random removal signifies failure or shut-down of a random component.

3.2 Flow Redistribution

Once a node has been removed, flows start to redistribute in the network. When a node is removed from the network, the incoming and outgoing links have certain loads that redistribute to the neighbours of the removed node.

Figure 4 illustrates the flow redistribution mechanism that we designed for re-routing power in case of a failure or an attack on a power grid. When node x is removed, all the incoming loads at node x are injected to its neighbouring nodes at the other end of the transmission links. Similarly, all the outgoing loads from node x are rejected from its neighbouring nodes at the other end of the

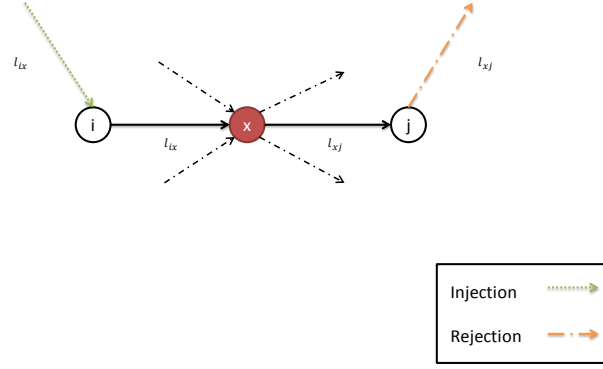


Fig. 4. Node N is removed from the network and flows redistribute to its neighbours

transmission links. It can be seen from Fig. 4 that the link carrying load l_{ix} will be removed from the network after node x has been removed and the load l_{ix} will be injected into node i . This procedure is applied to all the incoming neighbours i of node x . Similarly, for all the outgoing neighbours j of node x , a rejection of load l_{xj} occurs at each node j .

An injection makes sure that the load that was going into node x will now be redistributed to other parts of the network and a rejection allows for removing the excessive load from a part of the network that does not actually receive it any more.

A cumulative shift in load at each node is graphically shown in the flow redistribution part of the model in Fig. 2. Due to the numerous injections and rejections, loads at each node either increase or decrease and some might even change the direction of flow of power.

Using (1) we can deduce equations formulating injections and rejections for removal of node x as follows,

$$I = \sum_{i \in IN} l_{ix} \cdot u_i \quad , \quad (5)$$

$$R = \sum_{j \in ON} l_{xj} \cdot u_j \quad , \quad (6)$$

where IN and ON are sets of incoming and outgoing neighbours of x and u_i and u_j are $K \times 1$ column vectors specifying all row elements of the i^{th} and j^{th} column of the PTDF matrix, respectively. I and R are $K \times 1$ column vectors of

cumulative injections and rejections at every transmission link of the power grid due to removal of node x .

Using (5) and (6), we can state the following,

$$L_{NEW} = L_{OLD} + I - R \quad , \quad (7)$$

where L_{NEW} and L_{OLD} are $K \times 1$ column vectors specifying the loads at each transmission link.

After the initial trigger for simulating cascading failures, wherein we remove a node and all the incoming and outgoing links of *this* node from the network, the flow dynamics of the power grid change. We mark these nodes and links as out-of-service. As the next step, the model calculates the new loads for all the in-service transmission links. The loads flowing through each of the remaining nodes of the network are calculated by simply summing up all the incoming or outgoing loads of each node.

Each node may or may not have exceeded its capacity due to the possibility of extra incoming load. In (8) if the boolean statement S is true then at time t node i has exceeded its capacity and will be made out-of-service together with all its incoming and outgoing links.

$$S = \begin{cases} 1 & \text{if } L_i(t) > C_i \\ 0 & \text{otherwise} \end{cases} \quad , \quad (8)$$

As a result of rendering some nodes and their links out-of-service, some parts of the network may get disconnected and disintegrate into separate islands. Each island of the disintegrated network may or may not have generation substations. If an island is free of any generating source then it is dead, marked red in Fig. 5. However, if an island has a generating source, then we iterate the model on all such islands by removing all the nodes (together with their connected links) with the value of S as 1 or *true*, ie. overloaded nodes. Each island may result in an additional group of islands and the model is iterated on each group of islands belonging to the same time step simultaneously. This procedure can be encapsulated by a tree structure illustrated in Fig. 5.

Some islands may not be affected completely by flow redistribution, i.e. they still have a power generating source. In this case they are still functioning and are marked green in Fig. 5. Cascading effects have subsided in such islands and they are still providing energy for a part of their consumers. All the intermediate islands that could break down completely due to cascading failure are marked blue. The tree structure shows how an island (original power grid under consideration) can undergo changes in the flow of power and disintegrate into several islands some of which are functioning and some are deeply affected by the cascade.

At each time step of the simulation, a few nodes may get overloaded. The transition between simulation steps is assumed to be static as compared to a dynamic transient analysis where power flows mimic the real time taken for power to flow through a line with certain physical properties. Overloaded nodes

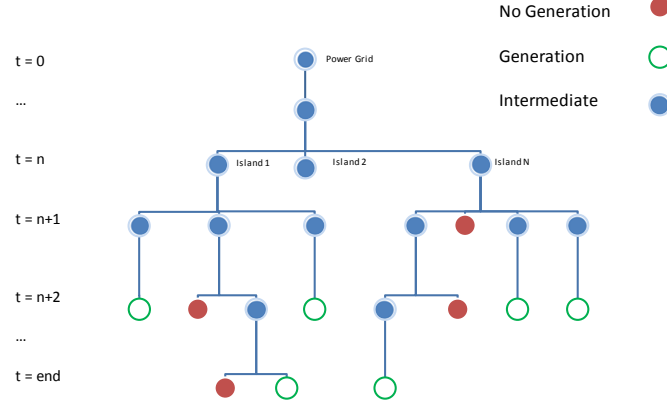


Fig. 5. A tree structure depicting the logical depth of the model and iterating procedure

are kicked out of the simulation all at once for any intermediate state of the simulation.

3.3 Output

We carry out simulations to observe the evolution of a cascade. The output of our model consists of several islands that may or may not be able to deliver power to their customers. At each time step a network is produced consisting of one or more disconnected components (islands). Every island contains information about the increase or decrease in load of each node belonging to that island. This group of disconnected islands is fed back as input to the model for the next time step after removing the overloaded nodes and connected links from the network. The flow redistribution model is iterated again on these group of islands. After processing this information from each time step we are able to assess the damage caused to the power grid.

4 Results

We followed a simulation based approach to solve our research problem. Simulations require an environment and the settings for that environment are defined in the next section followed by the approach used in the simulations and the discussion that stimulated from the results of our simulations.

4.1 Scenario

The scenario for carrying out our simulations is composed of three parts,

- Network Model

The main focus is on the high-voltage European power grid. This data consists of the topology and load settings of the grid and is available on-line from the database of Union for the Coordination of Transport of Electricity (UCTE) (UCTE n.d.). Apart from this we have also considered IEEE power system models ($N = 30, 39$, and 118) for comparison of a real power grid to synthetic network topologies.

- Node Removal Strategies

These strategies are based on centrality measures for nodes in a network. We focus on betweenness centrality, closeness centrality and degree centrality (Newman 2010) as theoretical measures from CNA to compare with node significance (Koç et al. 2013). We also analyse the network using an average of a hundred random removals. The distinction will be made wherever necessary.

- Tolerance Parameter

We have taken a realistic range of the tolerance parameter, $\alpha \in [1.01, 2.8]$ (3), in various settings. In reality this is different for each link/node of a network model that represents a power grid but for simplicity we have assumed a homogeneous loading level of the network, i.e. each node is loaded to the same percentage of its capacity.

4.2 Performance Measures

The following performance measures are used to assess the vulnerability of power grids,

- Damage 1 (D_1)

The fraction of nodes being overloaded at any time during a cascading failure represents the cumulative damage caused to a power grid at that point in time. This metric as a performance measure is very relevant to our work because a cascading failure propagates as a result of *overloading*.

- Damage 2 (D_2)

The fraction of energy demand that cannot be matched at any time during a cascading failure represents the cumulative damage caused to power grid users (consumers) at that point in time. This metric is relevant to our work because cascading failures directly affect the *consumers* of a power grid.

4.3 Simulations

We simulated our cascading failure model defined in Sect. 3 using proposed flow redistribution mechanism on the UCTE network model and other IEEE synthetic topologies. Cascading effects were observed for several removal strategies under different input parameter settings. To encapsulate a wide domain of

removal strategies we removed nodes with the highest betweenness centrality, degree centrality, closeness centrality and node significance separately and let the network mimic redistribution of flows that lead to a power outage if at all. For random failures and faults in the network, we removed a random node and averaged the damage caused by a hundred such removals. We used previously defined measures of *damage* to quantify the vulnerability of a power grid to cascading failures. We varied the tolerance parameter α and observed the evolution of D_1 and D_2 caused to the network. Note that each iteration of the simulation is counted as 1 time step.

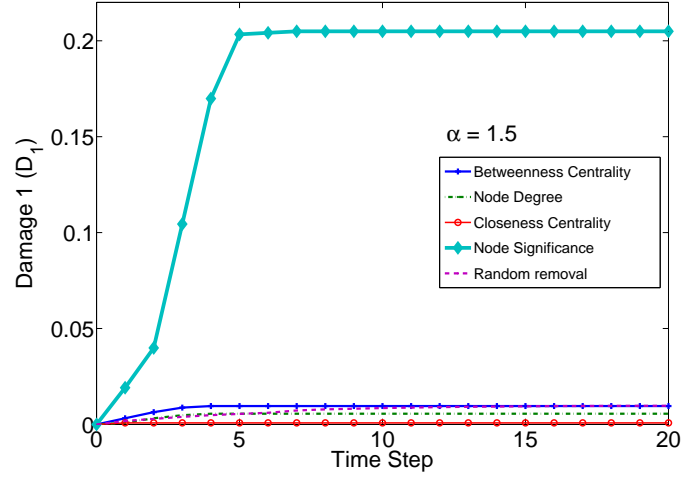
4.4 Discussion

Figure 6 shows a comparison of the damage caused by the five different removal strategies (of Subsect. 4.1), using the two ways to define damage (Subsect. 4.2) for a realistic loading level ($\alpha = 1.5$). We observe that the damage increased with time and after a certain point in time the effects stabilised. The two performance measures quantifying the damage (one in Fig. 6a and the other in Fig. 6b), show a similar trend. Therefore our conclusions do not depend on the chosen performance measure. As illustrated in Fig. 6, the damage caused by a removal strategy based on node significance results in approximately 20 times more damage compared to removal strategies based on the theory of CNA (Sect. 3.1). The attack strategies based on the traditional centrality measures even show less damage than random node removal does.

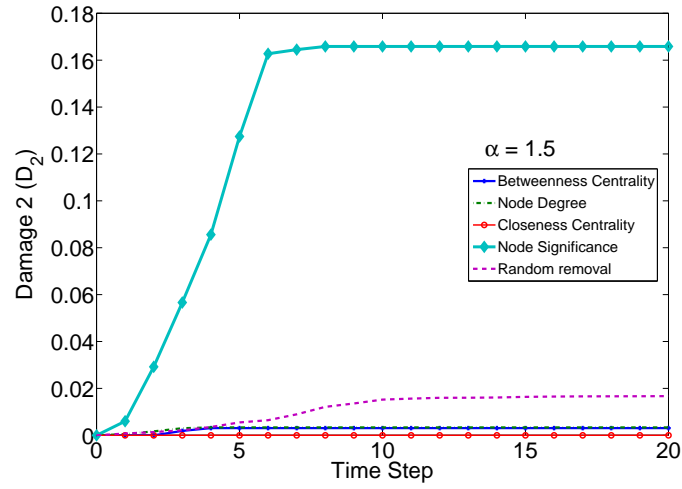
This shows that measures from CNA underestimate the vulnerability of a power grid to targeted attacks. Apparently, the removal strategies based on these measures do not attack the most important nodes in the grid. Therefore, these measures are not the best way to comment on the centrality of nodes in a power grid. Heuristically speaking, *node significance* may be an upper bound for the worst case damage caused to a power grid due to cascading failures. In order to focus on this worst case, i.e. the most disruptive removal strategy, we further concentrate on node significance.

Since both D_1 and D_2 plotted over time for a particular value of α are comparable to each other, we use only D_2 for expressing further results, i.e. fraction of unavailable energy. As expected, in Fig. 7, we see that the final damage after a cascading failure has subsided decreases with an increase in the tolerance parameter. The question now comes up how large the tolerance parameter should be in order to limit the damage to a given value. We address this question in Fig. 8 by plotting the total *damage* after cascading failure has subsided as a function of the tolerance parameter. It can be seen that the damage caused by cascading failures decreases by increasing the tolerance parameter, however, it is not a monotonically decreasing function. It behaves erratically for a small change in the tolerance parameter.

The reason for this erratic behaviour lies in the origin of flow redistribution. Each sub-station of the power grid is assumed to be homogeneously loaded at the beginning. Loads at each substation change after a failure or shut-down causes flows to redistribute. As a result each sub-station has a different threshold for



(a) Fraction of overloaded nodes



(b) Dissatisfied energy demand

Fig. 6. Comparison of damage caused over time for different removal strategies due to a cascading failure for $\alpha = 1.50$

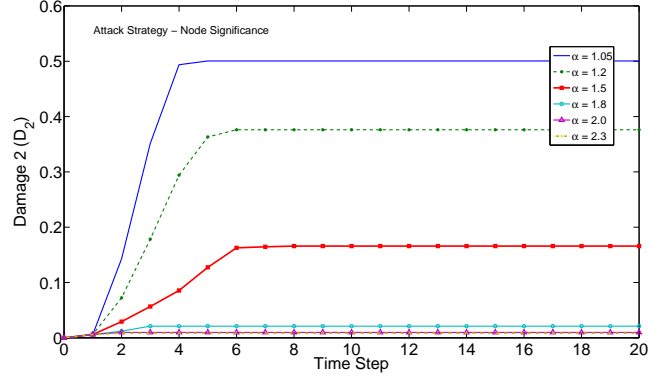
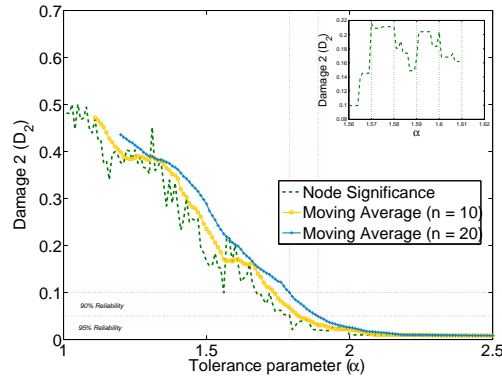
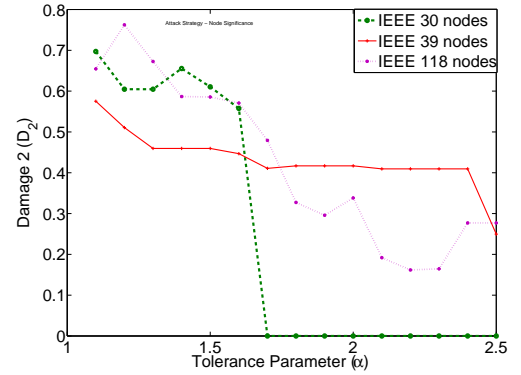


Fig. 7. Effect of load tolerance α on the damage caused to the system under a targeted attack based on node significance



(a) UCTE Network



(b) IEEE Synthetic topologies

Fig. 8. Final D_2 caused by removing the most significant node in the network for different values of tolerance parameter. The dotted lines in (a) represent reliability level of the system after a cascading failure has subsided, i.e. 90% reliability (10% damage) 95% Reliability (5% Damage).

breaking down. To illustrate this we take $\alpha = 1.56$ and remove a node with the highest node significance from the network. There are 21 nodes that get overloaded in the first time step. At $\alpha = 1.57$ there are 20 nodes that get overloaded in the first time step. Since the flows start redistributing after the first time step, this change in the number of overloaded nodes restructures the generation of islands and the redistribution takes different paths in different islands for these two values of α . Since we do not have reversible nodes, islands are generated because connectedness of the network cannot be kept intact after overloaded nodes go out-of-service. Therefore, the dynamics of flows change considerably for a very small change in the value of α (step increments of .01) as shown in Fig. 8a. We change the step increments to .001 and the inset of Fig. 8a shows that the damage curve becomes more erratic. To compare our results for a more generic overview, we plotted the final damage as a function of the tolerance parameter also for IEEE synthetic topologies. Figure 8b confirms our approach as in showing similar patterns of degradation in damage when capacity increases (α increases) for different topologies of synthetic IEEE networks.

To show the long-term trend we plotted a *simple moving average* of the damage caused at each step of the tolerance parameter. Simple moving average is the mean of previous z discrete data points. The curve represents the general long-term trend of reducing damage to a power grid by increasing the tolerance parameter. In Fig. 8a we have taken $z = 10$ data points and $z = 20$ data points. If we have more data points in the window of moving averages, we get a smoother relation between D_2 and α owing to the definition of moving averages itself. Hence, moving average is a good numerical approximation to show the intuitive relation between the destruction caused by a power outage and maximum capacity of power system components.

As can be seen in Fig. 8a, if we want to limit the damage to the European high-voltage power grid to 5–10% (90–95% reliability), a value of $\alpha = 1.79–1.89$ for the tolerance parameter would suffice. This implies that if each sub-station of the UCTE power grid is loaded to at most 55.8% (4) of its total capacity, the power grid will provide energy for at least 90% of its consumers, even if an attack targeted to the most vulnerable node is carried out.

5 Conclusions

5.1 Summary

We used a simulation based approach to implement a flow redistribution mechanism that takes into account the underlying flow characteristics of power grids. We continued the research by analysing the vulnerability of the European high-voltage power grid using our enhanced model. This analysis involved a study of the damage to the grid caused by a node removal based on the highest centrality for four centrality measures: betweenness, closeness, node degree and node significance. We carried out a comparison based on these four removal strategies and an average of a hundred random removals. In the analysis ‘damage’ is

measured in terms of number of overloaded nodes and the percentage of energy demand that could not be satisfied.

As expected, the removal of a random node caused less damage than a targeted attack for node significance. Surprisingly, this was not the case for the other centrality measures. Our studies show that the theoretical centrality measures (betweenness, closeness and node degree) underestimate the vulnerability of power grids to cascading failures in comparison with node significance, which is a context based measure. Removing a node with the highest node significance causes remarkably more damage than removing a node with the highest centrality (betweenness/closeness/degree). This shows that node significance is more suitable than the traditional centrality measures for finding the most vulnerable nodes in a power grid.

A second result that we obtained by using our model for flow redistribution is the quantification of the needed tolerance level in the European high-voltage power grid in order to limit the damage caused by targeted attacks. If approximately eighty percent of spare capacity is available for each node (with respect to the typical node loading level), then a removal of the most vulnerable node (that is the node with highest node significance) causes at most ten percent of damage (measured in amount of dissatisfied energy demand).

By modelling flow redistribution in a realistic manner, we have developed a way to identify the vulnerable nodes in a power grid and to determine the node capacity that is needed to guarantee a certain level of robustness against targeted attacks. In addition, we showed that centrality of nodes in power grids should not be defined based on topological network properties only; the power flowing through the grid should be considered when defining centrality in the context of power grids.

5.2 Future Work

We examined cascading failures in power grids and wrote a detailed comparison between different centrality measures. A logical next step is to expand the typography and include more centrality measures related to link capacities and optimised flow distribution. A detailed investigation in entropy based centrality measures will also be helpful in understanding the vulnerability of power grids.

Furthermore, transient dynamic analysis of power flow can be explored for a more real-time behaviour. So far we have assumed that transition from one simulation stage to the next is discrete. Using the temporal behaviour of power flow through transmission lines will be a step closer to reality.

We also assume that the links are loaded homogeneously. An effort towards using real capacities of power components instead of estimates with tolerance parameter would provide for a more accurate study.

Concerning applications to the industry, with minor changes to input parameters and a suitable replacement for power distribution this model can be applied to low voltage segments to investigate their structural vulnerabilities as an initiative towards *smart-grids*.

Acknowledgements

This work is funded by the NWO project RobuSmart: Increasing the Robustness of Smart Grids through distributed energy generation (a complex network approach), grant number 647.000.001.

References

- Albert, R., Albert, I. & Nakarado, G. L. (2004), ‘Structural vulnerability of the north american power grid’, *Physical Review E* **69**, 025103.
- Albert, R., Jeong, H. & Barabási, A.-L. (2000), ‘Error and attack tolerance of complex networks’, *Nature* **406**, 378–382.
- Arianos, S., Bompard, E., Carbone, A. & Xue, F. (2009), ‘Power grids vulnerability: a complex network approach’, *Chaos* **19**, 013119.
- Asztalos, A., Sreenivasan, S., Szymanski, B. K. & Korniss, G. (2012), ‘Distributed flow optimization and cascading effects in weighted complex networks’, *The European Physical Journal B-Condensed Matter and Complex Systems* **85**, 1–10.
- Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D.-U. (2006), ‘Complex networks: structure and dynamics’, *Physics Reports* **424**, 175–308.
- Bompard, E., Gao, C., Masera, M., Napoli, R., Russo, A., Stefanini, A. & Xue, F. (2007), ‘Approaches to the security analysis of power systems: Defence strategies against malicious threats’, *Luxembourg: Office for Official Publications of the European Communities*.
- Bompard, E., Masera, M., Napoli, R. & Xue, F. (2009), ‘Assessment of structural vulnerability for power grids by network performance based on complex networks’, *Critical Information Infrastructure Security* **5508**, 144–154.
- Bompard, E., Napoli, R. & Xue, F. (2009), ‘Analysis of structural vulnerabilities in power transmission grids’, *International Journal of Critical Infrastructure Protection* **2**, 5 – 12.
- Bompard, E., Napoli, R. & Xue, F. (2010), ‘Extended topological approach for the assessment of structural vulnerability in transmission networks’, *Generation, Transmission Distribution, IET* **4**, 716 –724.
- Bompard, E., Wu, D. & Xue, F. (2010), The concept of betweenness in the analysis of power grid vulnerability, in ‘Complexity in Engineering, 2010. COMPENG’10.’, IEEE, pp. 52–54.
- Borgatti, S. P. (2005), ‘Centrality and network flow’, *Social Networks* **27**, 55–71.
- Callaway, D. S., Newman, M. E., Strogatz, S. H. & Watts, D. J. (2000), ‘Network robustness and fragility: Percolation on random graphs’, *Physical Review Letters* **85**, 5468–5471.
- Cohen, R., Erez, K., Ben-Avraham, D. & Havlin, S. (2000), ‘Resilience of the internet to random breakdowns’, *Physical review letters* **85**, 4626–4628.
- Crucitti, P., Latora, V. & Marchiori, M. (2004), ‘Model for cascading failures in complex networks’, *Physical Review E* **69**, 045104.
- Dobson, I., Greene, S., Rajaraman, R., DeMarco, C. L., Alvarado, F. L., Glavic, M., Zhang, J. & Zimmerman, R. (2001), ‘Electric power transfer capability: Concepts, applications, sensitivity, uncertainty’, *PSERC Publication* pp. 01–34.
- Kinney, R., Crucitti, P., Albert, R. & Latora, V. (2005), ‘Modeling cascading failures in the north american power grid’, *The European Physical Journal B* **46**, 101.

- Koç, Y., Warnier, M., Brazier, F. M. T. & Kooij, R. E. (2013), A robustness metric for cascading failures by targeted attacks in power networks, *in* 'In proceedings of the 10th IEEE International Conference on Networking, Sensing and Control (ICNSC'13)'.
- McLinn, J. (2009), 'Major power outages in the us, and around the world', *IEEE Reliability Society*.
- Mitchell, M. (2009), *Complexity : A Guided Tour*, Oxford University Press.
- Motter, A. E. & Lai, Y.-C. (2002), 'Cascade-based attacks on complex networks', *Physical Review E* **66**, 065102.
- Nasiruzzaman, A. B. M. & Pota, H. R. (2011), 'Transient stability assessment of smart power system using complex networks framework', *CoRR* pp. 1–7.
- Newman, M. (2010), *Networks: An Introduction*, Oxford University Press, Inc.
- Pahwa, S., Hodges, A., Scoglio, C. & Wood, S. (2010), Topological analysis of the power grid and mitigation strategies against cascading failures, *in* 'Systems Conference, 2010 4th Annual IEEE', IEEE, pp. 272–276.
- Purchala, K., Meeus, L., Van Dommelen, D. & Belmans, R. (2005), 'Usefulness of dc power flow for active power flow analysis', *IEEE Power Engineering Society General Meeting 2005* **1**, 2457–2462.
- Rosas-Casals, M., Valverde, S. & Solé, R. V. (2007), 'Topological vulnerability of the european power grid under errors and attacks', *International Journal of Bifurcation and Chaos* **17**, 2465–2475.
- Simonsen, I., Buzna, L., Peters, K., Bornholdt, S. & Helbing, D. (2008), 'Transient dynamics increasing network vulnerability to cascading failures', *Physical review letters* **100**, 218701.
- Tutzauer, F. (2007), 'Entropy as a measure of centrality in networks characterized by path-transfer flow', *Social Networks* **29**, 249 – 265.
- UCTE (n.d.), 'European high-voltage dataset', <https://www.entsoe.eu/the-association/history/ucte/>.
- Van Eeten, M., Nieuwenhuijs, A., Luijff, E., Klaver, M. & Cruz, E. (2011), 'The state and the threat of cascading failure across critical infrastructures: The implications of emperical evidence from media incident reports', *Public Administration* **89**, 381–400.
- Youssef, M., Scoglio, C. & Pahwa, S. (2011), Robustness measure for power grids with respect to cascading failures, *in* 'Proceedings of the 2011 International Workshop on Modeling, Analysis, and Control of Complex Networks', ITCP, pp. 45–49.
- Zimmerman, R. (n.d.), 'Matpower simulation package', <http://www.pserc.cornell.edu/matpower/>.